Lamphills

# Data Breach Response Plan Template

## Data breach response plan

Crisis management team’s role

### STEP 1: Assign a crisis management team consisting of:

CEO

Chair

Other key staff (business manager, deputy, IT, etc.)

### STEP 2: Agree on the role of each crisis management team member.

Roles could include writing communications, making phone calls, researching accurate information etc. The most important role is that of the final approver of all decisions.

### STEP 3: Agree on the need for meetings:

how often to meet and for how long, e.g., 30 minutes twice a day

what information will be brought to the meetings, and how will they run who will chair them?

Remember, the situation will be changeable, so ensure meetings provide opportunities to share updates.

## STEP 4: Establish what has happened.

Complete the data breach list for either third parties or internal systems.

## STEP 5: Agree on a communications plan, which should establish:

who to communicate with

how to communicate

who should do the communicating

who has approval and sign-off.

## STEP 6: Take action.

A template letter is included. Include as much information as possible without breaching anyone’s confidentiality or privacy.

Third-party breach plan

This plan outlines the actions [organization name] will take during a data breach at a third-party provider (e.g. SurveyMonky, Zoom). Complete as many boxes as necessary.

| Name of third-party provider | Data held | [Organisation name’s] response if a breach occurs |
|---|---|---|
| E.g. SurveyMonkey | email addresses<br>demographic data (e.g. age, country of birth) | Security officer tracks breach<br>Security officer logs on to the platform to understand the scope of data breached<br>CEO prepares to field questions from the public<br>CEO publishes statement on organisation's website<br>CEO writes to affected people (if contact details are known) |

| | | |
|---|---|---|
| E.g., Zoom | email addresses<br>faces (personal information)<br>information or opinions expressed about individuals (maybe)<br>intellectual property or confidential information that is not personal information, but could be in breach of confidentiality clauses in the organisation's agreement and terms of use | As above |

Organization breach plan

This plan outlines the actions [organisation name] will take in the event that its own systems are breached. Complete as many boxes as necessary.

| Type of data held | Where it is held | What has been breached | Response plan |
|---|---|---|---|
| Volunteers' personal information:<br>name<br>address<br>date of birth<br>phone number<br>email address<br>location/program of volunteering<br>notes<br>number of hours volunteered | Customer relationship management (CRM) database | Inappropriate access to the CRM has been identified | IT officer identifies how breach occurred.<br>IT officer closes further access to data.<br>IT officer identifies potentially affected individuals.<br>CEO writes to individuals potentially affected detailing what data may have been disclosed, and the organisation's actions in response. |

Communications plan

This plan details which communications will take place and who is responsible for them. Complete as many boxes as necessary.

| Person/group to be contacted | How to communicate | Who to communicate |
|---|---|---|
| Staff | Phone / email / website / press release / social media? | CEO? Chair? Closely connected staff member? |

| | |
|---|---|
| Volunteers | Phone / email / website / press release / social media? |
| Individuals affected | Phone / email / website / press release / social media? |
| Broader community | Phone / email / website / press release / social media? |
| Wider audience which does not have any connection to your organisation | Phone / email / website / press release / social media? |

| Communications | Responsibility for writing/speaking | Responsibility for approving |
|---|---|---|
| Letter to affected people | | CEO and Chair |
| Letter to staff | | CEO and Chair |
| Letter to volunteers | | CEO and Chair |
| Statement for website | | CEO and Chair |

| | |
|---|---|
| Quotes in case of media contact | CEO and Chair |
| Media interviews | CEO and Chair |
| Statement on social media | CEO and Chair |

## Data breach response letter template

Dear

Institute of Community Directors Australia

(This is member-only content; use but please don't distribute)

DISCLAIMER: While all care has been taken in the preparation of this material, no responsibility is accepted by the author(s) or Our Community, its staff, volunteers or partners, for any errors, omissions or inaccuracies. The material provided in this resource has been prepared to provide general information only. It is not intended to be relied upon or be a substitute for legal or other professional advice. No responsibility can be accepted by the author(s) or Our Community or its partners for any known or unknown consequences that may result from reliance on any information provided in this publication.

Page 5

Lamphills

I am writing to let you know about a recent data breach at [organisation name] involving some of your personal information. This letter explains what happened, how we have responded and what it means for you.

[On/between] [date/time period], [provide a summary of the incident and why it constitutes a breach]

We have shut down the affected systems and we are working to identify exactly what data has been disclosed and who is affected. This will take some time, but as soon as we have more information, we will be in contact with you again. However, I wanted to let you know about this incident as soon as possible.

At this stage, we believe the “worst case scenario” is that [personal information about all our volunteers has been accessed illegally: name, address, date of birth, phone number, email address, location of volunteering, number of hours volunteered, and notes recorded by our volunteer coordinator.]

Your privacy is important to us, and I would like to personally apologise for any distress this incident causes. I assure you that the team at [organisation] is working hard to prevent it from happening again. I greatly value your contribution to our organisation, and our whole community benefits from the work that you do.

The Office of the Australian Information Commissioner has published a detailed guide on how individuals can reduce the risk of harm from data breaches (for example, by changing passwords). For more information, please visit www.oaic.gov.au/privacy/data-breaches/respond-to-a-data-breach-notification. I urge you to consider implementing the precautions outlined there.

If you don’t have access to the Internet and you would like a copy of the guide mailed to you, please contact my office on (0X) 000 0000.

As I mentioned, I will be in touch again as soon as I have more details about this incident. In the meantime, for the latest information about our ongoing investigation into the data breach, please visit our website: [insert URL].

[Organisation]'s programs and operations are continuing as normal, including our volunteer programs.

Yours sincerely,

CEO, [organisation]

Chair/President, [organisation]